UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/963,659	09/27/2001	Ivan Teblyashkin	550-272	9245

23117 7590 08/05/2005

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/963,659	TEBLYASHKIN ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5,7-9,11-14,16,17,19-21,23-26,28,29,31-33,35 and 36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-2,4-5,7-9,11-14,16-17,19-21,23-26,28-29,31-33,35-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-2,4-5,7-9,11-14,16-17,19-21,23-26,28-29,31-33,35-36 have been considered.

Drawings

New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are illegible. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2,4-5,7-9,11-14,16-17,19-21,23-26,28-29,31-33,35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yann, U.S. Patent Application Publication No. 2002/0078368, in view of Risch, U.S. Patent No. 5,471,629, in further view of Nachenberg, U.S. Patent No. 6,357,008.

As per claims 1,13, and 25, the applicant describes a method of detecting a computer virus comprising the following limitations which are met by Yann in view of Risch in further view of Nachenberg:

a) analysis logic operable to analyse program instructions forming said executable computer program to identify suspect program instructions forming said executable computer program to identify suspect program instructions being one or more of:

i) a program instruction generating a result value not used by another portion of said executable computer program;

ii) a program instruction dependent upon an uninitialised variable (Yann: [0030]);

b) detecting logic operable to detect said executable computer program as containing a computer virus if a number of suspect program instructions identified for said executable computer program exceeds a threshold level (Yann: [0030]; [0016]);

c) wherein said analysis logic includes a dependency table indicating a dependency between state variables within said computer and loaded variable values, and for each program instruction said analysis logic makes a determination as to which state variables are read and written by that program instruction and for each loaded variable value within said dependence table if any state variable read by that program instruction is marked as dependent upon said loaded variable value, then all state variables written by that program instruction are marked as dependent upon said loaded variable value with previous dependencies being cleared (Yann: [0030], [0034]; Risch: Col 10, lines 28-51);

d) analysis logic parses said executable computer program for suspect program instructions by following execution flow and upon occurrence of a branch first following a first branch path having saved pending analysis results and subsequently returning to follow a second branch path having restored said pending analysis results (Nachenberg: Col 10, line 3 to Col 11, line 25)

Yann discloses all the limitations of parts a and b. Yann also discloses the limitation of part c with the exception that Yann does not disclose the use of storing the data in a table. Risch teaches the well-known idea that data may be stored in a table. More specifically, Risch discloses the use of a dependency table in which parameters and associated values are monitored. It would have been obvious to one or ordinary skill in the art at the time the invention was filed to combine the ideas of Risch in view of Yann and store data in a table because doing so provides a convenient way for a system to store and monitor data.

Yann in view of Risch disclose all the limitations of parts a through c. However, Yann in view of Risch fail to disclose part d. Nachenberg discloses an anti-virus system which, like the applicant's system and Yann's system, seeks to provide protection against polymorphic viruses through heuristic analysis.

Nachenberg teaches a system which analyzes a target computer program for suspect program instructions by following execution flow and upon occurrence of a first branch point following the first branch. Nachenberg also discloses that the system saves pending analysis results when it takes a branch point since the system saves both the destination address of the untaken branch and the state of the CPU emulator (ie associated registers, etc) (Col 10, lines 37-52). When the system finishes executing the branch, it subsequently returns to follow the second branch and it restores the pending analysis results. Nachenberg comments that it is important to save the pending analysis results (ie the state of CPU emulator at the time the branch was taken) so that a proper analysis of the second branch can ensue (Col 10, line 53 to Col 11, line 25) and the execution can accurately exhibit the operation of the code.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nachenberg with those of Yann in view of Risch because doing so provides an additional method to analyze a target program and determine if it is a polymorphic virus. A system which incorporates the ideas of Nachenberg is more robust and provides greater security because it can detect a polymorphic virus by analyzing a dependency table to acknowledge redundant code operations and/or by following the branch path execution of the potential polymorphic virus.

As per claims 2,14, and 26, the applicant describes the computer program product of claims 1,13, and 25, which are met by Yann in view of Risch in further view of Nachenberg, with the following limitation which is also met by Yann:

Wherein said computer virus is a polymorphic computer virus ([0030]);

As per claims 4,16, and 28, the applicant describes the computer program product of claims 1,13, and 25, which are met by Yann in view of Risch in further view of Nachenberg, with the following limitation which is also met by Yann:

Wherein for each program instruction said analysis logic is operable to make a determination as to which state variables are read by that program instruction ([0034]);

The applicant should note that the variables read by the program instruction are labeled as being in a "used" state. The applicant should also note that program instructions are evaluated on a one-by-one basis ([0031]).

As per claims 5,17, and 29, the applicant describes the computer program product of claims 1,13, and 25, which are met by Yann in view of Risch in further view of Nachenberg, with the following limitation which is also met by Yann:

Wherein for each program instruction said analysis logic is operable to make a determination as to which state variables are written by that program instruction ([0035]);

The applicant should note that the variables written by the program instruction are labeled as being in a "set" state.

As per claims 7,19, and 31, Yann discloses the computer program product of claims 3,15, and 27, which are met by Yann in view of Risch in further view of Nachenberg, with the following additional limitation which is also met by Yann:

Wherein said state variables include one or more of:

(i) register values;

(ii) processing result flag values;

(iii) a flag indicative of a write to a non-register storage location ([0034]).

As per claims 8,20, and 32, the applicant describes the computer program product of claims 1,13, and 25, which are met by Yann in view of Risch in further view of Nachenberg, with the following limitation which is also met by Yann:

Wherein said analysis logic is operable to maintain an initialization table indicating which state variables have been initialized ([0033],[0034], and 24 of Fig 2);

Uninitialized variables are labeled "undefined". Initialized variables are labeled as "set" if written to or "used" if in a used state.

As per claims 9,21, and 33, the applicant describes the computer program product of claims 8,20, and 32, which are met by Yann in view of Risch in further view of Nachenberg, with the following additional limitation which is also met by Yann:

Wherein a state variable is marked as initialized upon occurrence of any one of:

(i) a write to said state variable of a determined initialized value; and

(ii) use of said state variable as a memory address value by a program instruction ([0034]).

As per claims 11,23, and 35, the applicant describes the method of claims 10,22, and 34, which are met by Yann in view of Nachenberg (see above), with the following limitation which is met by Nachenberg:

Wherein a branch path stops being followed when any one of:

(i) there are no further suitable program instruction for execution within that branch path; and

(ii) said branch path rejoins a previously parsed execution path (Col 10, lines 26-36);

As per claims 12,24, and 36, the applicant describes the computer program product of claims 1,13, and 25, which are met by Yann in view of Risch in further view of Nachenberg, with the following additional limitation which is also met by Yann:

Wherein if said threshold level is exceed, then further virus detection mechanisms are triggered to confirm the presence of a computer virus ([0016]).

Response to Arguments

Applicant's arguments, see Remarks filed 7/5/05 with respect to claims 1,13, and 25 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to claims 11,23, and 35 have been fully considered but they are not persuasive. The applicant's remarks are irrelevant to the rejection. The applicant requests that

the examiner provide support for his official notice stance on claims 11,23, and 35. The rejection was not made with regard to official notice.

The rejection was made in light of part (ii) of the limitation being taught by Nachenberg. The examiner also indicated in the action that part (i) was inherent in Nachenberg.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER